

Figure 1

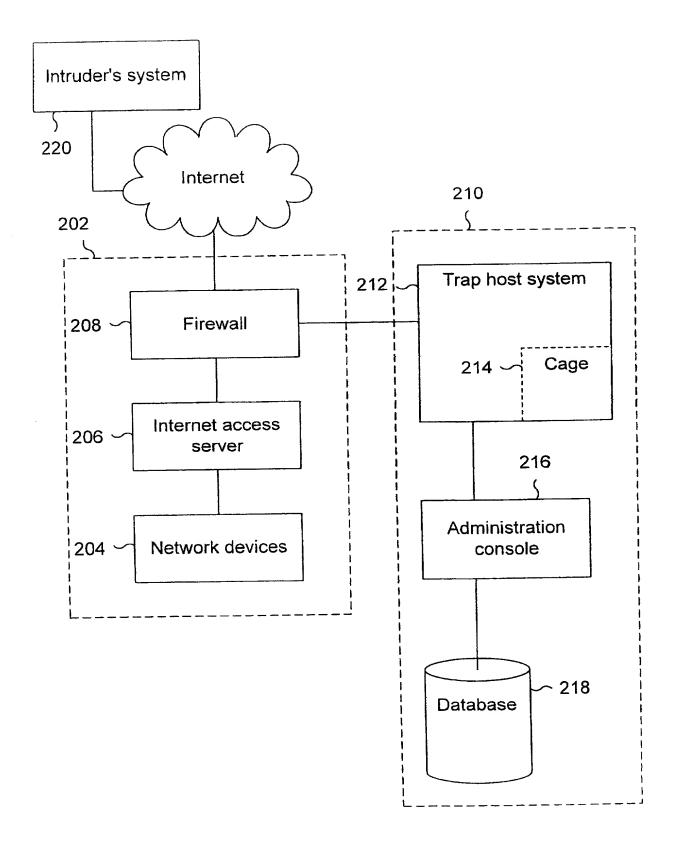


Figure 2

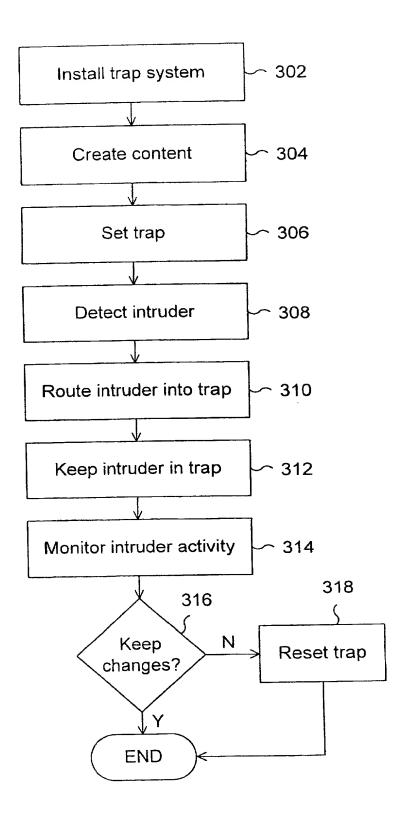


Figure 3

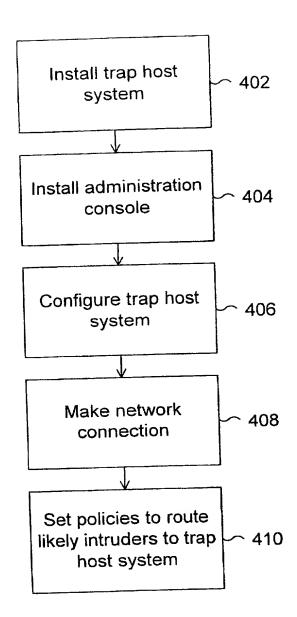
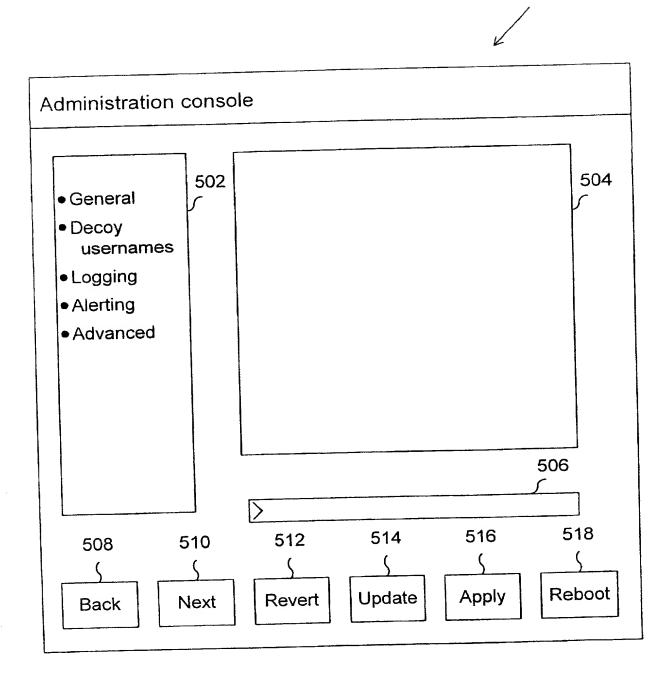


Figure 4



500

Figure 5

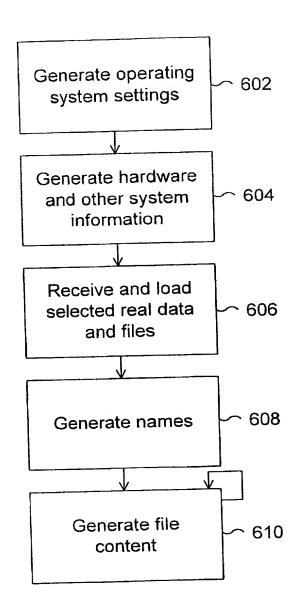


Figure 6

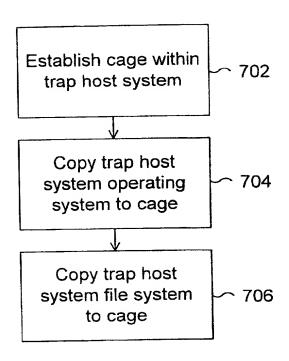


Figure 7

Connect Edit Termina Help
Sun0S 5.7
NOTICE TO USERS
Use of this system constitutes consent to security monitoring and testing. By using this system, the user consents to any interception, monitoring, recording, copying, auditing, inspection, or disclosure at the descretion of authorized site or corporate personnel.
Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in the warning.
login:

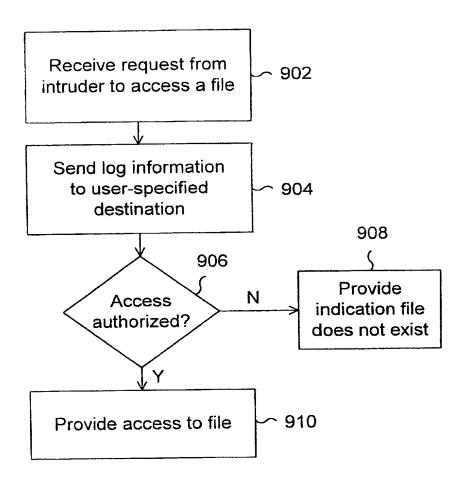


Figure 9

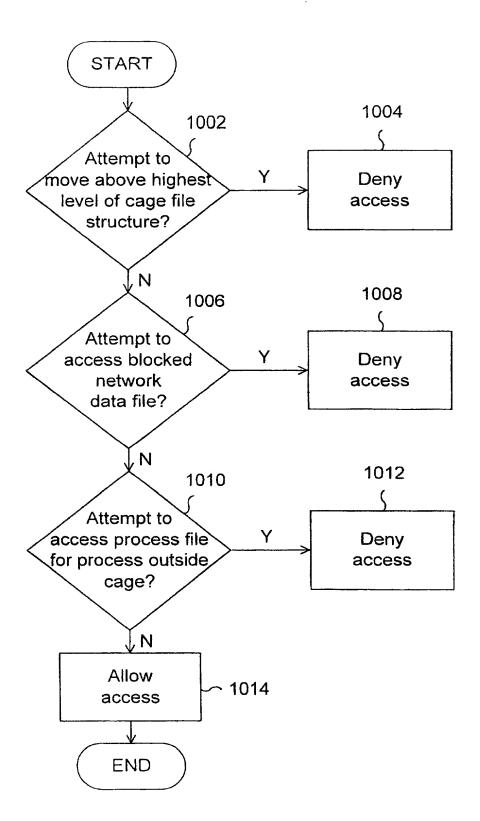


Figure 10

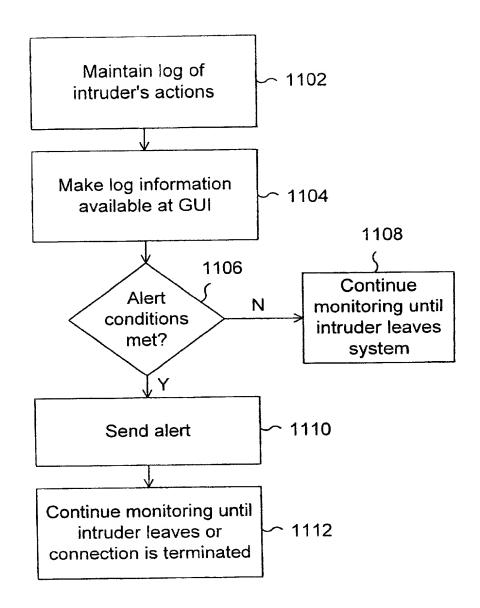


Figure11A

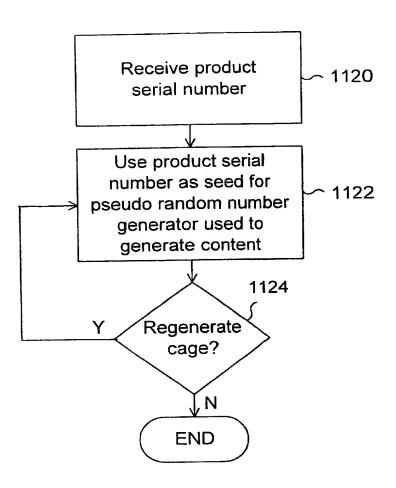


Figure 11B

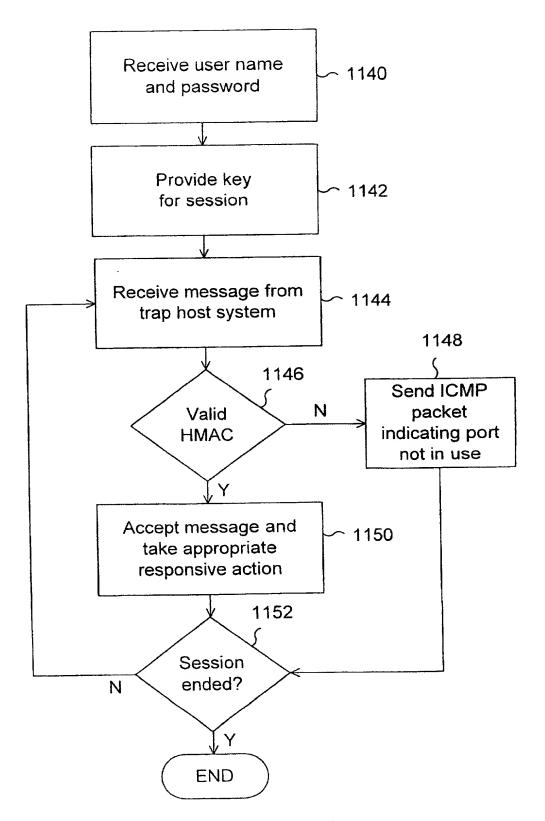


Figure11C

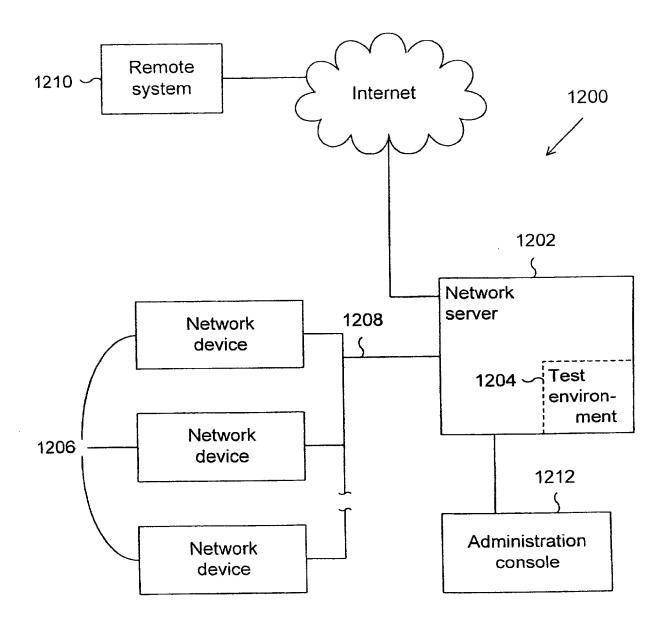


Figure 12

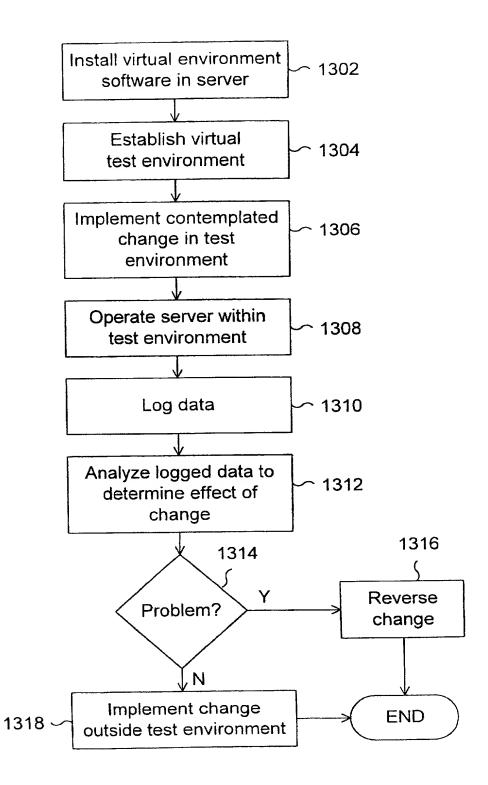


Figure 13

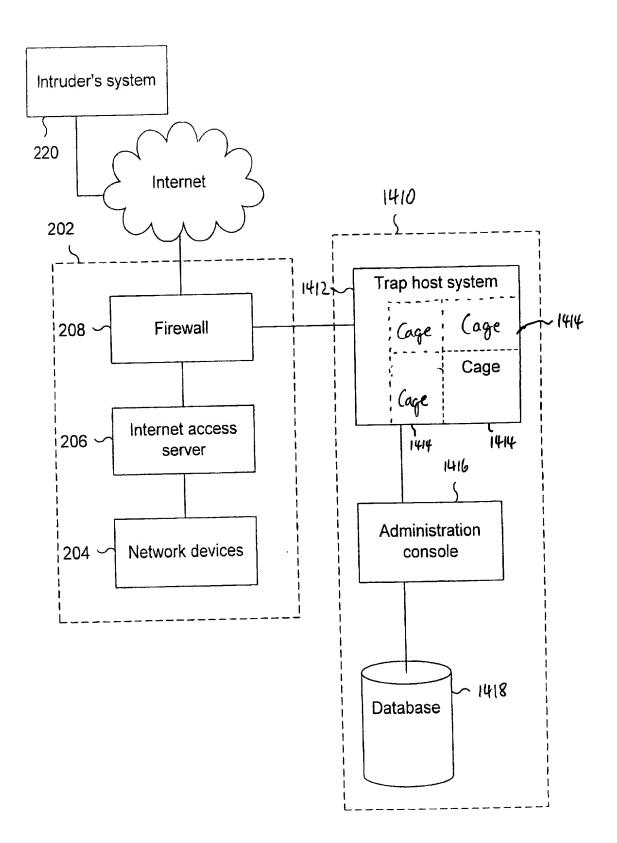


Figure 14

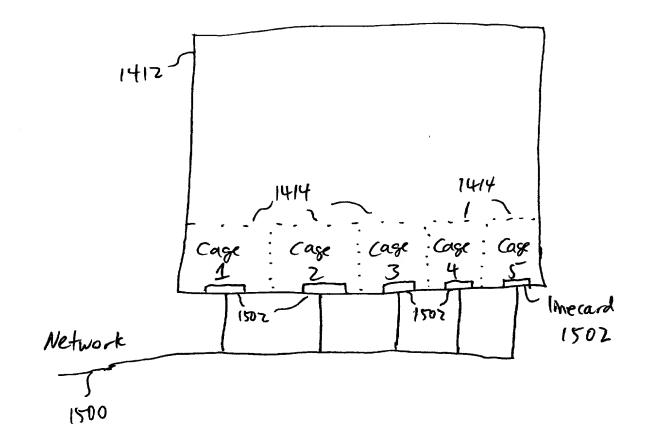
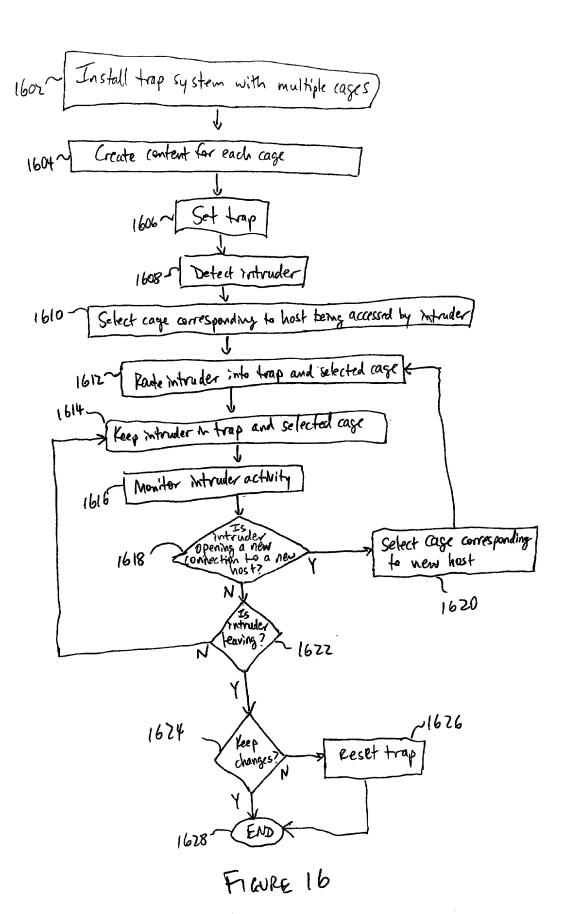


Figure 15



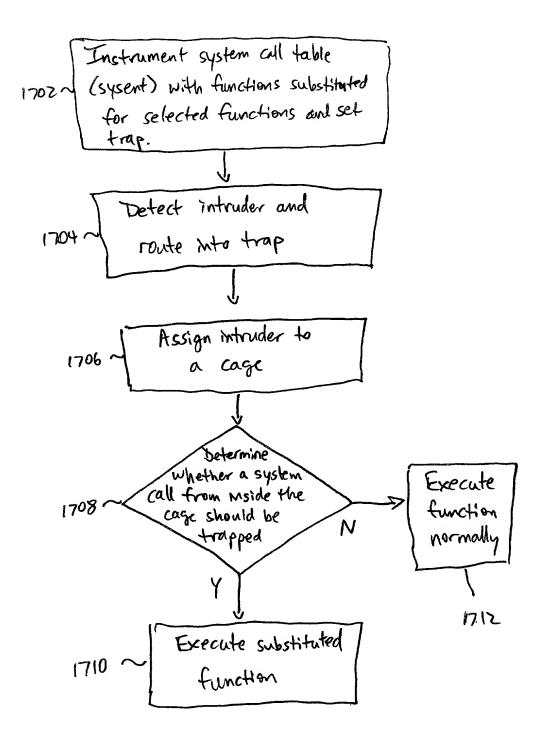


Figure 17

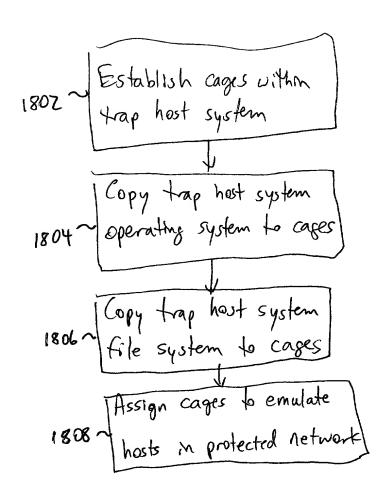


Figure 18

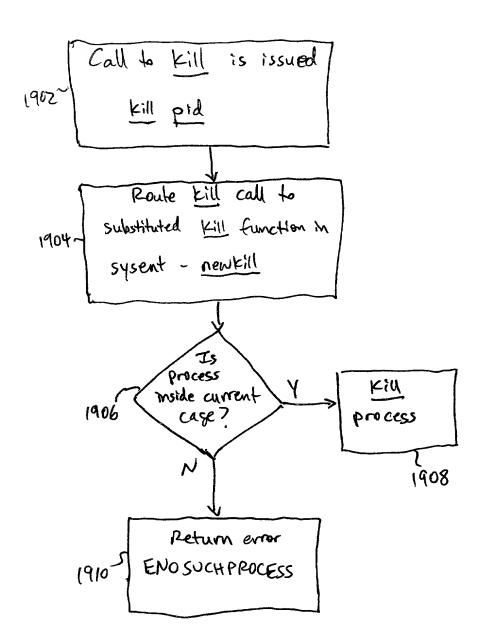


Figure 19

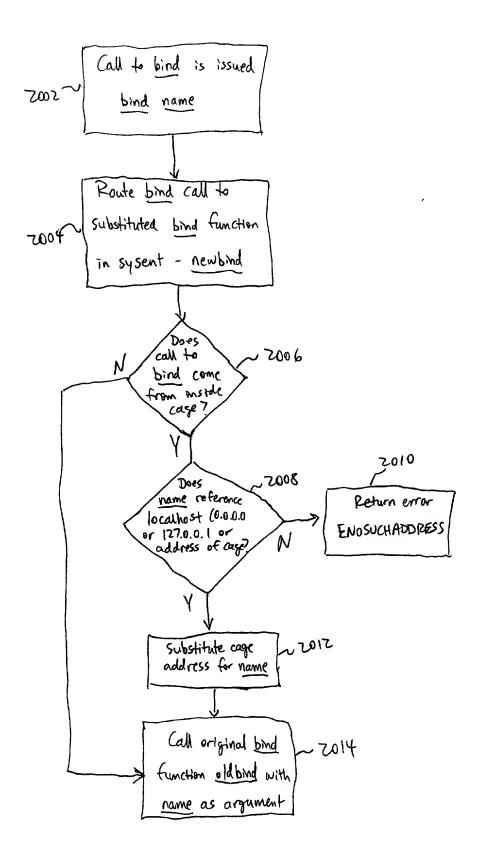


Figure 20

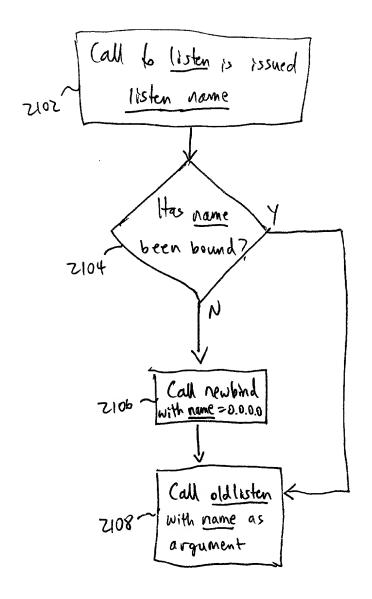


Figure 21

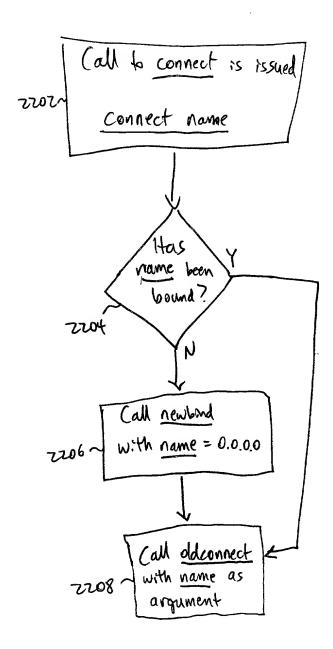


Figure 22

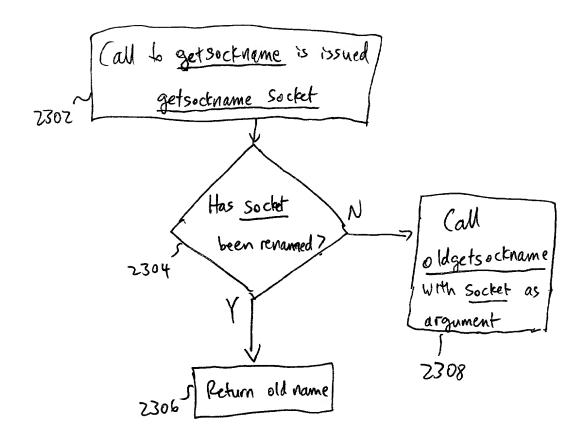


Figure 23

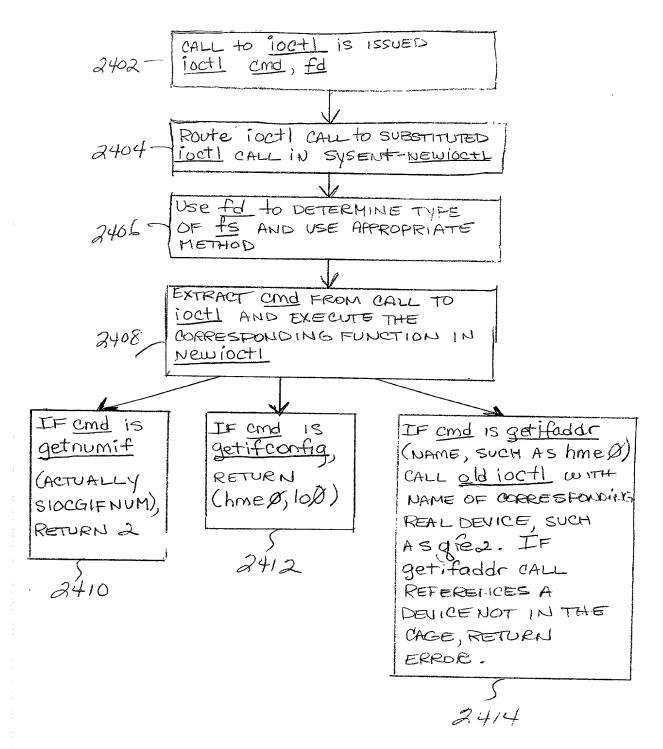


FIGURE 04

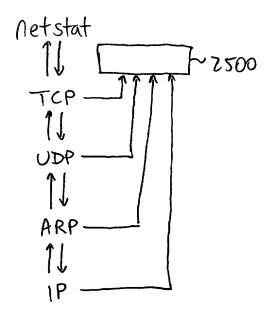


Figure 75

```
<doc>
<regexp-query>
      <name>Possible SGID Exploit
      properties>
           <priority>10</priority>
      </properties>
      <pattern>
           <line>.*exec args=.*pid=\((\\d+\)); ppid=\(\\d+\); uid=\(\\d+\); euid=
\(\d+\); gid=\([1-9]\d*\); egid=\(0\).*</line>
           </next>
           <next>
           <line>.*args=\([\-\w\\\/ ]+\); pid=\(\\d+\); ppid=\(\%1\%\).*</line>
           </next>
     </pattern>
      cmatch>
           <actionpair>
                 ine>.*args=\(([\-\w\\\/]+)\).*ppid=\(%1%\).*</line>
                 <action>
                       <highlight/>
                       <delete/>
                       <varop var="agg">%1%</varop>
                 </action>
           </actionpair>
     <annotation>
           <text>Possible SGID Exploit: %agg%</text>
     </annotation>
</regexp-query>
</doc>
```

```
<doc>
      <regexp-query>
      <name>Possible SUID Exploit
      cproperties>
             <priority>10< /priority>
      </properties>
      <pattern>
             <next>
             <line>.*exec args=.*pid=\((\d+)\); ppid=\((\d+\); uid=\([1-9]\d*\);
euid=\(0\).*</line>
             </next>
             <next>
             \langle line \rangle.*args = \langle (.+ \rangle); pid = \langle (d+ \rangle); ppid = \langle (%1% \rangle).* \langle /line \rangle
      </pattern>
      cmatch>
             <actionpair>
                    <line>.*args=\(.+)\); pid=\(\d+\); ppid=\(%1%\).*</line>
                    <action>
                           <highlight/>
                           <delete/>
                           <varop var="agg">%1%</varop>
                    </action>
       </procmatch>
       <annotation>
              <text>Possible SUID Exploit: %agg%</text>
       </annotation>
</regexp-query>
</doc>
```

```
<doc>
<regexp-query>
     <name>All Processes</name>
     cproperties>
           <priority>10</priority>
     </properties>
     <pattern>
           <next>
           <line>.*proclog.*args=\(([\-\.\w\\\/ ]+)\).*</line>
     </pattern>
     cmatch>
           <actionpair>
                 <line>.*args=\(([\-\.\w\\\/ ]+)\).*</line>
                 <action>
                       <highlight/>
                       <delete/>
                       <varop var="agg">%1%</varop>
                 </action>
           </actionpair>
      <annotation>
            <text>Process started: %agg%</text>
      </annotation>
</regexp-query>
</doc>
```

```
<doc>
<regexp-query>
      <name>Find Processes...</name>
      properties>
             <priority>10</priority>
      </properties>
      <args>
             <args>.+</args>
             <ppid>\d+</ppid>
             \langle uid \rangle \langle d+ \langle /uid \rangle
             <euid>\d+</euid>
             \langle gid \rangle \langle d+\langle /gid \rangle
             <egid>\d+</egid>
      </args>
      <pattern>
             <line>.*args=\(%args%\); pid=\(%pid%\); ppid=\(%ppid%\);
uid=\(%uid%\); euid=\(%euid%\); gid=\(%gid%\); egid=\(%egid%\).*</line>
             </next>
      </pattern>
      cmatch>
             <actionpair>
                    <line>.*args=\((.+)\); pid.*</line>
                    <action>
                          <highlight/>
                          <delete/>
                          <varop var="agg">%1%</varop>
                   </action>
             </actionpair>
      </procmatch>
      <annotation>
             <text>Process started: %agg%</text>
      </annotation>
</regexp-query>
</doc>
```

```
<doc>
<regexp-query>
      <name>All Shell-spawned Processes
      properties>
           <priority>l0</priority>
     </properties>
      <pattern>
           <line>.*exec args=\(-sh\); pid=\((\\d+)\).*</line>
           </next>
           <next>
           <line>.*args=\(([\-\w\\\/ ]+)\).*ppid=\(%1%\\.*</line>
     </pattern>
     cmatch>
           <actionpair>
                 <line>.*args=\(([\-\w\\\/ ]+)\).*ppid=\(%1%\).*</line>
                 <action>
                       <highlight/>
                       <varop var="agg">%l%</varop>
                 </action>
           </actionpair>
     </procmatch>
     <annotation>
           <text>Executed from a shell: %agg%</text>
     </annotation>
</regexp-query>
</doc>
```

Figure 30

```
<doc>
<regexp-query>
      <name>Incoming Connections</name>
      properties>
            <priority>10</priority>
      </properties>
      <pattern>
            <next>
            <line>.*incoming connection from=\(.+\).*</line>
      </pattern>
      cmatch>
            <actionpair>
                  <line>.*incoming connection from=\((.+):(.+)\)
to=\((.+):(.+)\).*</line>
                  <action>
                         <highlight/>
                         <delete/>
                        <varop var= "fromip">%1%</varop>
                        <varop var= "fromport">%2%</varop>
                        <varop var= "toip">%3%</varop>
<varop var= "toport">%4%</varop>
                  </action>
            </actionpair>
      <annotation>
            <text>Incoming Connection From IP: %fromip% (on port: %fromport%) To
IP: %toip% (on port: %toport%)</text>
      </annotation>
</regexp-query>
</doc>
```

```
<doc>
<regexp-query>
     <name>Keystrokes Entered</name>
     cproperties>
           <priority>10</priority>
     </properties>
     <pattern>
           <next>
           <line>.*read stream data, id=\((\\d+)\) data=\\(.+\\).*</line>
           </next>
           <next fromprev="1">
           <line>.*read stream data, id=\(%1%\) data=\(.*\\0[ad4].*\).*</line>
           </next>
     </pattern>
     cmatch>
           <actionpair>
                  <line>.*read stream data, id=\(%1%\) data=\((.+)\).*</line>
                  <action>
                        <highlight/>
                        <delete/>
                        <varop var="agg">%1%</varop>
                  </action>
           </actionpair>
     </procmatch>
      <annotation>
            <text>Keystrokes Entered: %agg%</text>
     </annotation>
</regexp-query>
</doc>
```

```
<doc>
<regexp-query>
      <name>Screen Output</name>
      cproperties>
            <priority>10</priority>
      </properties>
      <pattern>
            <next>
            <line>.*write stream data, id=\((\d+)\) data=\(.+\).*</line>
            </next>
            <next fromprev="1">
            <line>.*write stream data, id=\(%1%\)
data=\(.*\\0[ad46].*\).*</line>
            </next>
      </pattern>
      cmatch>
            <actionpair>
                  <line>.*write stream data, id=\(%1%\) data=\((.+)\).*</line>
                  <action>
                        <highlight/>
                        <delete/>
                        <varop var="agg">%1%</varop>
                  </action>
           </actionpair>
     </procmatch>
     <annotation>
           <text>Output to screen: %agg%</text>
     </annotation>
</regexp-query>
</doc>
```

Figure 33

```
<doc>
<regexp-query>
      <name>Find Monitored</name>
      properties>
           <priority>10</priority>
      </properties>
      <args>
           <file name>.+</file name>
           </args>
      <pattern>
           <next>
           <line>.*monitored file opened name=\(%file_name%\)
pid=\(%pid%\).*</line>
           </next>
      </pattern>
      cmatch>
           <actionpair>
                 <line>.*monitored file opened name=\((.+)\)
pid=\((.+)\).*</line>
                 <action>
                       <highlight/>
                       <delete/>
                       <varop var="filename">%1%</varop>
                       <varop var="pidvar">%2%</varop>
                 </action>
           </actionpair>
     <annotation>
           <text>File Opened: %filename% (from pid: %pidvar%)</text>
     </annotation>
</regexp-query>
</doc>
```